POLICY

Behandling av personuppgifter

Syfte

Syftet med denna policy avseende behandling av personuppgifter är att medvetandegöra att behandling av personuppgifter inom Assessio-koncernen (nedan Assessio) sker på ett sådant sätt att det är förenligt med dataskyddslagstiftningen.

Bakgrund

Assessio behandlar löpande personuppgifter såväl om kunder, kandidater och om personal som andra, exempelvis samarbetspartners. Vår utgångspunkt är att inte behandla fler personuppgifter än vad som behövs för aktuellt ändamål, och vi strävar alltid efter att använda de minst integritetskänsliga uppgifterna.

Grundläggande förutsättningar

För all behandling av personuppgifter måste två förutsättningar vara uppfyllda. Dels måste det finnas en laglig grund för behandlingen, och dels måste behandlingen ske i enlighet med de grundläggande principerna.

Det finns huvudsakligen fem lagliga grunder som kan komma ifråga.

- Samtycke av den registrerade
- För att fullgöra avtal
- Det följer av lag
- Nödvändigt för att skydda intressen som är av grundläggande betydelse för den registrerade eller annan fysisk person
- Intresseavvägning.

Förutom att någon eller några av dessa grunder måste vara tillämpliga för att personuppgifter ska kunna behandlas, måste all behandling ske med upprätthållande av följande sex grundläggande principer.

- Principen för laglighet, korrekthet och öppenhet
- Principen om ändamålsbegränsning (och finalitetsprincipen)
- Principen för uppgiftsminimering
- Principen om riktighet
- Principen om lagringsminimering, och
- Principen för integritet och konfidentialitet

Riktlinjer

Personuppgifter

Assessio behandlar endast personuppgifter när det föreligger laglig grund. De vanligaste lagliga grunderna för vår behandling av personuppgifter är att uppgifterna behövs för att fullgöra förpliktelser enligt avtal och lag.

Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Enligt dataskyddsförordningen kallas den första principen för laglighet, korrekthet och öppenhet (eng. lawfulness, fairness and transparency).

1. Lagligheten innebär att behandlingen av personuppgifter måste vara i enlighet med bestämmelserna i dataskyddsförordningen och tillhörande reglering som gäller personuppgifter. Begreppet laglighet återfinns exempelvis i dataskyddsförordningens bestämmelse att en personuppgiftsansvarig måste ha en laglig grund för behandlingen av personuppgifter.
2. Varje behandling av personuppgifter ska vara laglig och rättvis. Det ska vara klart och tydligt för fysiska personer hur personuppgifter som rör dem insamlas, används, konsulteras eller på annat sätt behandlas samt i vilken utsträckning personuppgifterna behandlas eller kommer att behandlas.
3. En korrekt behandling förutsätter att de registrerade får kännedom om behandlingen, dvs. att de informeras i enlighet med regleringen i dataskyddsförordningen.
4. Öppenhet innebär att all information som ska lämnas till den registrerade och all kommunikation i samband med behandlingen av dessa personuppgifter, t.ex. om den registrerade begär ett registerutdrag, är lättillgänglig och lättbegriplig samt att ett klart och tydligt språk används. Den principen gäller framför allt informationen till registrerade om den personuppgiftsansvariges identitet och syftet med behandlingen.

Ändamålet med behandlingen

Varje behandling av personuppgifter ska ha uttryckligt angivna och berättigade ändamål. Personuppgifterna får inte behandlas på ett sätt som är oförenligt med dessa ändamål. De särskilda ändamål som personuppgifterna behandlas för ska vara tydliga och legitima och ha bestämts vid den tidpunkt då personuppgifterna samlades in. Att begränsa ändamålet för behandlingen av personuppgifter framgår av de grundläggande principerna (principen om ändamålsbegränsning).

Ändamålen måste bestämmas redan när uppgifterna samlas in och det måste anges uttryckligen. Det finns inte någon möjlighet att skjuta upp bestämmandet av ändamålet till ett senare tillfälle. Ändamål kan endast i begränsad omfattning läggas till efteråt.

Information till den registrerade

Enligt Dataskyddsförordningen ska information lämnas till de registrerade om bl.a. den lagliga grunden för behandlingen av personuppgifterna. Detta gäller oavsett om personuppgifterna kommer från den registrerade själv eller inte, dvs. om de har erhållits från någon annan.

Information ges bland annat på hemsidan, i aktuella avtal, och i Assessios allmänna villkor.

Behandling på betryggande sätt

Rätten att ta del av och hantera personuppgifter är begränsad inom Assessio. Personal etc har endast rätt att ha tillgång till och hantera sådana personuppgifter som vederbörande behöver för att utföra sina arbetsuppgifter.

I fråga om känsliga personuppgifter har Assessio inrättat särskilda behörighetskontroller, vilket innebär ett högre skydd för dessa personuppgifter.

Våra säkerhetssystem är utvecklade med integritet i fokus och skyddar i mycket hög grad mot intrång, förstöring samt andra förändringar som kan innebära en risk för enskilds integritet.

Vi överför inte personuppgifter i andra fall än de som uttryckligen anges i denna policy.

Överföring av personuppgifter

Assessio lämnar inte ut personuppgifter om det inte är nödvändigt för att uppfylla förpliktelser enligt avtal eller lag. Personuppgifter kan också i förekommande fall överföras till Assessios leverantörer. I fall då personuppgifter lämnas ut till tredje part upprättas sekretessavtal samt säkerställs att personuppgifterna även i övrigt behandlas på ett betryggande sätt.

Personuppgiftsansvar

Assessio ingår personuppgiftsbiträdesavtal såväl avseende de fall där Assessio är personuppgiftsansvarig, som i de fall där Assessio är personuppgiftsbiträde.

I fall där Assessio använder leverantörer av IT-lösningar där personuppgifter behandlas (exempelvis molnlösningar) träffas personuppgiftsbiträdesavtal mellan Assessio och den aktuella leverantören.

Uppgiftsminimering och gallring

Personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (principen för uppgiftsminimering).

Personuppgifter ska inte hanteras på ett sätt som är mer omfattande än vad som fordras för de ändamål för vilka de behandlas, dvs vad som är nödvändigt för de ändamål som de behandlas för. En viktig del av detta är att tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum (se även principen om lagringsminimering nedan). Assessio samlar varken in mer eller mindre personuppgifter, eller ovidkommande uppgifter, än vad som verkligen behövs i förhållande till ändamålet med behandlingen. Det ska vara möjligt att förklara varför de olika uppgifterna behövs för att uppfylla ändamålen med behandlingen. Personuppgifter som inte längre är nödvändiga för att uppnå ändamålet, ska gallras genom att raderas. Inom Assessio använder standardtider för kontroll och i förekommande fall radering av personuppgifter. Dessa tider fastställas för varje system/personuppgiftsflöde.

Löpande kvalitetsarbetet

Att tillse att behandling av personuppgifter görs på ett sätt som följer vid var tid gällande lagstiftning, utgör en del av Assessios löpande kvalitetsarbete. Det innebär bl a att denna Policy för behandling av personuppgifter, samt andra policys, rutiner och processer löpande ses över och hålls uppdaterade. Vidare ingår det i det löpande kvalitetsarbetet att tillse att de grundläggande principerna efterlevs, genom att exempelvis kontrollera att personuppgifter inte hanteras på andra sätt än för uppgivet ändamål, att uppgifter inte lagras längre eller i större omfattning än vad som fordras etc.